AO 106 (Rev. 04/10) Application for a Search Warrant AUSA Mangan

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the cellular device assigned with call number 305-877-8162 and/or IMSI 310150922236083 in the custody or control of AT&T

Case No. 2:18-mj-704

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A - This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41.

located in the Unknown District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1029	Access device fruad
18 USC 1030(a)	Fraud and related activity in connection with computers

The application is based on these facts:

See attached Affidavit. To ensure technical compliance with 18 U.S.C. §§ 3121-3127, the requested warrant will also function as a pen register order. I thus certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by FBI. See 18 U.S.C. §§ 3122(b), 3123(b).

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Seth Erlinger, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/17/2018

Judge's signature

City and state: Columbus, Ohio

Hon. Elizabeth Preston Deavers, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF INORMATION ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED WITH 305-877-8162 AND/OR INTERNATIONAL MOBILE SUBSCRIBER IDENTITY NUMBER 310150922236083, THAT IS IN THE CUSTODY OR CONTROL OF AT&T	Case No 2:18-mj-704 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Seth Erlinger, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular device assigned with number **305-877-8162** ("the SUBJECT ACCOUNT"), with listed subscriber(s) **Luis Daniel Trujillo Conde** or **Daniel Conde**, that is in the custody or control of **AT&T**, a wireless communications service provider that is headquartered at **11760 U.S. Highway 1, Suite 600, North Palm Beach, FL 33408**. As a provider of wireless communications service, **AT&T** is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15). This affidavit is sought to renew a search warrant obtained on July 31, 2018 (Case No. 2:18-MJ-566).

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require AT&T to disclose to the government the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

3. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. See 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. See 18 U.S.C. § 3123(b)(1).

4. I am a Special Agent with the Federal Bureau of Investigation, and have been since September 2017. I am currently assigned to the Cincinnati Field Office, Cyber Crime Squad, which is responsible for investigating computer and high-technology crimes, and I am trained and authorized to investigate the offenses alleged herein. Since my assignment to the Cyber Crime Squad, I have received both formal and informal training from the FBI regarding cyber investigations.

5. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1029 (access device fraud) and 18 U.S.C. § 1030 (computer intrusion) have been committed by Luis Daniel Trujillo Conde, Dennis Frank Fernandez Miyares, and as-yet unidentified co-conspirators. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

7. The Court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court

of the United States that has jurisdiction over the offense being investigated; *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. The United States government, including the FBI, is investigating skimmer devices placed on gas station pumps around the Southern District of Ohio. The investigation concerns possible violations by Luis Daniel Trujillo Conde ("Conde"), Dennis Frank Fernandez Miyares ("Miyares"), and as-yet unidentified co-conspirators of, inter alia, 18 U.S.C. § 1029 (access device fraud) and 18 U.S.C. § 1030 (computer intrusion).

9. On May 24, 2018, the Ohio State Highway Patrol conducted a traffic stop in Madison County, OH along I-70 of a white 2018 Chevrolet Suburban bearing a Georgia license plate. The vehicle was identified as a rental vehicle, and inside the vehicle the trooper found two males, Conde and Miyares. Conde informed the trooper they had travelled from Miami to Cleveland, and were driving credit cards for a friend from Dayton to Columbus. The trooper later determined the names on some of the cards recovered from the vehicle did not match the names present on the magnetic strips. The subjects were also found to be in possession of a suspected skimmer device and a laptop computer. Conde provided the trooper with telephone number 305-877-8162 as his contact number.

10. Pursuant to a 2703(d) order, AT&T provided subscriber information, historical call detail records, and cell tower connections for telephone number 305-877-8162. The subscriber for number 305-877-8162 was identified as Daniel Conde. Conde has been an AT&T subscriber since October 2016, and has held the phone with MSISDN 305-877-8162 since March 26, 2018.

11. Analysis of the AT&T data lead to the discovery on June 21, 2018 of a skimming device placed on a gas station pump in northern Columbus, Ohio. An examination of the skimmer revealed a MAC address that had also been paired via Bluetooth with the laptop recovered by the Ohio State Highway Patrol.

12. On July 9, 2018, the FBI interviewed a Columbus, Ohio-based individual (Victim #1) whose debit card had been compromised and used at a Home Depot, also on the north side of Columbus, in an attempt to purchase a gift card. Victim #1 stated he had only used that card once, on June 10, 2018, at the same gas station and pump where the skimmer device was recovered on June 21, 2018.

13. Pursuant to a Grand Jury subpoena, Alamo Rent-a-Car provided information regarding a reservation made by Conde for the period of June 7 through June 11, 2018. Conde provided email address trujilloconde@yahoo.es and telephone number 305-877-8162 as his contact information.

14. Pursuant to a Grand Jury subpoena, FedEx provided information regarding packages sent and received by Conde. The records revealed Conde sent a package on June 10, 2018 from Columbus, Ohio to an address in Miami, Florida.

15. Historical Cell Site Location Information (CSLI) for telephone number 305-877-8162 obtained via search warrant revealed Conde traveled to the Washington, DC metro area four times between June and July 2018. Historical CSLI for telephone number 305-877-8162 obtained via the search warrant also revealed Conde traveled to the Columbus, Ohio area On June 8, 2018 and June 28, 2018.

16. On July 31, 2018, the FBI obtained a prospective cell site location information (CSLI) warrant related to the phone number 305-877-8162.

17. On August 15, 2018, Conde's email address, trujilloconde@yahoo.es, received seven emails from Expedia.com. On August 17, 2018, through the prospective CSLI obtained via search warrant, the FBI identified Conde at Ronald Reagan International Airport in Arlington, VA.

18. Between August 17, 2018 and August 20, 2018, CSLI indicated Conde traveled extensively around Northern Virginia, and as far south as the Charlottesville, VA area.

19. On September 6, 2018, Conde's email address, trujilloconde@yahoo.es, received four emails from Expedia.com. On September 10, 2018, through the prospective CSLI obtained via search warrant, the FBI identified Conde at Ronald Reagan International Airport in Arlington, VA. On September 10, 2018, FBI physical surveillance observed Conde drive a rental vehicle to a BP gas station in Woodbridge, VA. Conde remained next to a pump for approximately seven minutes before driving away, without exiting the vehicle.

20. On September 13, 2018, at the request of law enforcement, the owner of the BP gas station in Woodbridge, VA facilitated an inspection of the pumps. No skimmer was found.

21. Also on September 10, 2018, FBI physical surveillance observed Conde entering two different home center stores in central Virginia. Conde made three trips into the first store, and two trips into the second store. Conde was observed changing clothing between trips into the stores.

22. On September 11, 2018, FBI physical surveillance observed Conde entering four different home center stores in central and southern Virginia. Conde made eight total trips into the four stores, and changing clothes between trips into stores he visited more than once.

23. Continued prospective cell site information will aid the FBI in detecting and investigating the criminal activity in which Luis Daniel Trujillo Conde is engaged. Specifically,

as the subject travels around the United States to install, service, and otherwise engage in skimming-related activities, cell site information will provide the FBI with details on locations Conde is likely engaged in such activity.

24. In my training and experience, I have learned that AT&T is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

25. Based on my training and experience, I know that AT&T can collect cell-site data on a prospective basis about the SUBJECT ACCOUNT. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as AT&T typically collect and retain cell-site data pertaining to cellular devices to which

they provide service in their normal course of business in order to use this information for various business-related purposes.

26. Based on my training and experience, I know that AT&T also can collect Network Event Location System, which AT&T also refers to as "NELOS". NELOS data estimates the approximate distance of the cellular device from a cellular tower based upon the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

27. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content. Currently, the SUBJECT PHONE has MSISDN 305-877-8162 and IMSI 310150922236083.

28. Based on my training and experience, I know that wireless providers such as AT&T typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers

such as AT&T typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT ACCOUNT's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

29. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. The proposed warrant will also function as a pen register order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and/or trap and trace device to record, decode, and/or capture certain information in Attachment A for each communication to or from the SUBJECT ACCOUNT, without geographic limit, for a period of forty-five days (45) days pursuant to 18 U.S.C. § 3123(c)(1).

30. I further request that the Court direct AT&T to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on AT&T, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

31. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents

because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

Seth Erlinger
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on September 17, 2018

UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular device assigned **MSISDN 305-877-8162 and/or IMSI 310150922236083** ("the SUBJECT ACCOUNT"), with listed subscriber **Luis Daniel Trujillo Conde or Daniel Conde,** that is in the custody or control of **AT&T**, a wireless communications service provider that is headquartered at **11760 U.S. Highway 1, Suite 600, North Palm Beach, FL 33408.**

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. Information associated with each communication to and from the SUBJECT ACCOUNT for a period of **45 days from the date of this warrant**, including:

   i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

   ii. Source and destination telephone numbers;

   iii. Date, time, and duration of communication; and

   iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the SUBJECT PHONE will connect at the beginning and end of each communication as well as Network Event Location System data (also known as "NELOS").

b. For the period of **July 31, 2018 to the date of this warrant**, all records and other information (not including the contents of communications) relating to wire and

electronic communications sent or received by the SUBJECT ACCOUNT, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received), as well as Network Event Location System data (also known as "NELOS").

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. § 1029 (access device fraud) and 18 U.S.C. § 1030 (computer intrusion) involving **Luis Daniel Trujillo Conde** during the period **October 2016 to the date of this warrant**.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by AT&T, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of AT&T. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of AT&T, and they were made by AT&T as a regular practice; and

b. such records were generated by AT&T electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of AT&T in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by AT&T, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature